1. GENERAL INFORMATION

A. The Department collects sensitive information to include personal identifying information (PII), such as private information, government-issued identifiers, financial account information as well as restricted City information (RCI) as defined by Administrative Regulation (AR) 1.90, Information Privacy and Protection.

B. The Department is committed to protecting the confidentiality, integrity, and availability of information collected, stored, maintained, and used in carrying out its efforts to protect the public and suppress criminal activity.

C. This policy establishes procedures for Department personnel in order to comply with departmental, city, state, and federal requirements which govern information privacy and protection.

D. All Department personnel play a critical role in maintaining the Department's information privacy and protection standards as well as the highest degree of public trust.

2. ACCESS CONTROLS

A. Authorization

(1) Sensitive information should only be accessed by authorized personnel in order to perform specific job-related responsibilities or assignments.

(2) Each work unit is responsible for restricting and controlling access to Department computing systems and hard copy information based on a need-to-know basis.

(3) Sensitive information should only be accessed by authorized third parties in order to perform specific job-related responsibilities or assignments.

- Each work unit is responsible for ensuring all third-party verifications, data security agreements, and required contract provisions have been completed prior to sharing PII and/or RCI with a third party.

B. Physical Security - Each work unit is responsible for managing physical access to Department computing systems and hard copy information.

C. Network Security - Each work unit is responsible for managing microcomputer access to Department computing systems.

3. COLLECTION AND USE OF PII AND/OR RCI

A. Sensitive information should only be collected for its stated purpose and must be directly related to the carrying out of the Department's authorized activities.

B. The storage of PII and/or RCI on any unencrypted storage device, such as universal serial buses (USBs), compact discs (CDs), or external hard drives, is prohibited.

- Work units having a legitimate business need to store PII and/or RCI must use encrypted USBs, CDs, external hard drives, etc.

C. Work units will exercise the utmost precaution when collecting full social security numbers (SSNs) and take appropriate measures to restrict disclosure of full SSNs unnecessarily.

D. Work units which accept credit/debit cards are responsible for ensuring reasonable steps are taken to comply with payment card industry (PCI) standards.

3. D. Record Management - Each work unit is responsible for collecting and maintaining sensitive information in accordance with AR 1.61, Records Management Program.

- Department designated records control officers (RCOs) will assist work units to:

  * Conduct periodic reviews in order to limit or eliminate collection and/or storage of redundant or unnecessary PII and/or RCI
  * Adhere to City retention schedules
  * Dispose of sensitive information that is deemed no longer necessary

E. Secure Transmissions - Work units will exercise the utmost precaution when transporting or transmitting PII and/or RCI and take appropriate measures to restrict transporting of paper format and transmitting of electronic format PII and/or RCI unnecessarily.

4. **TRAINING**

A. Each work unit is responsible for ensuring authorized personnel receive training regarding information privacy and protection that corresponds to specific job-related responsibilities or assignments.

(1) City of Phoenix Information Security Awareness Training - Awareness training to instruct City personnel on how to protect City data and prevent information security breaches.

(a) Required training by all City personnel at time of hire and annually thereafter

(b) Provided by the City Information Security and Privacy Office (ISPO) in accordance with AR 1.84, Information Security Management

(2) Criminal Justice Information Services (CJIS) Training - Awareness training to instruct authorized personnel on CJIS security policy requirements for handling criminal justice information (CJI).

(a) Required training by all authorized personnel whose job duties require access to CJI at time of hire and bi-annually thereafter

- Should be completed at the same time as bi-annual Terminal Operator Certification (TOC)

(b) Provided by the Arizona Department of Public Safety (DPS) and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division

- TOC and CJIS Training are overseen by the Strategic Information Bureau's Data Integrity Unit

(3) 28 Code of Federal Regulations (CFR) Part 23 Guidelines Training - Introductory level training which provides an understanding of privacy and civil liberties concerns related to multijurisdictional criminal intelligence systems.

5. **INFORMATION SECURITY AND PRIVACY ASSESSMENT (ISPA)**

A. In order to comply with AR 1.90, Information Privacy and Protection, the Department will develop, assess, and document all PII and RCI collected, stored, maintained, and used, as well as, the security measures used to protect this information.

B. The Department's designated information security liaison will implement and oversee an annual assessment to include:

(1) Identification of all Department PII and RCI, regardless of format

5. B. (2) Identification and review of current Department security measures which ensure information privacy and protection regarding authorized use:

- Within the Department
- Within the City
- With authorized third-party external businesses and law enforcement partners

(3) Identification and review of current Department policies which address information privacy and protection

(4) Identification and review of current records management procedures to eliminate the collection and/or storage of redundant or unnecessary information

(5) Identification and review of current Department training which focuses on information privacy and protection

(6) Completion of an annual IMP Report to be presented to executive staff for review and submission to the ISPO

6. **RELATED POLICIES AND STANDARDS** - The below related policies and/or standards apply to the listed section/s of this order.

RELATED POLICY OR STANDARD	SECTION/S OF THIS ORDER
• AR 1.61, Records Management Program	• 3.D – Record Management
• AR 1.63, Electronic Communications and Information Acceptable Use	• 2.E – Network Security
• AR 1.64, City Policy on Cellular Equipment and Service	• 2.E – Network Security
• AR 1.73, Control of Communications Services and Systems	• 2.E – Network Security
• AR 1.84, Information Security Management	• 2.A – Authorization • 2.B – Third Party Authorization • 2.E – Network Security • 3.A – Collection and Use of PII and/or RCI • 5 – Information Security and Privacy Assessment (ISPA)
• AR 1.90, Information Privacy and Protection	• 2.A – Authorization • 2.E – Network Security • 3.A – Collection and Use of PII and/or RCI • 5 – Information Security and Privacy Assessment (ISPA)
• AR 1.91, Information Privacy and Protection Supplement – Data Shared with Third Parties	• 2.A – Authorization • 2.E – Network Security • 5 – Information Security and Privacy Assessment (ISPA)
• AR 1.95, Privacy Program	• 2.A – Authorization • 5 – Information Security and Privacy Assessment (ISPA)
• AR 3.96, Merchant Accounts (Payment Card Processing)	• 3.C – Collection and Use of PII and/or RCI
• AR 4.44, Contract Worker Identification and Access Controls	• 2.D – Physical Security
• AR 4.45, Contract Worker Background Screening	• 2.A – Authorization
• Information Technology (IT) Standard b1.4, Information Management Plan	• 5 – Information Security and Privacy Assessment (ISPA)

6. **RELATED POLICIES AND STANDARDS** - (Continued)

SECTION/S OF THIS ORDER	RELATED POLICY OR STANDARD
• IT Standard s1.12 – Handling Confidential Information	• 2.A – Authorization • 2.D – Physical Security • 2.E – Network Security • 3.A – Collection and Use of PII and/or RCI • 3.E – Secure Transmission
• IT Standards1.7, Media Retention and Removal	• 3.A – Collection and Use of PII and/or RCI • 3.E – Secure Transmission
• Operations Order 3.9.00, Police Facilities	• 2.A – Authorization • 2.D – Physical Security
• Operations Order 5.4.00 & 5.4.A Employee Software and Internet User Agreement	• 2.E – Network Security
• Police Headquarters Security and Parking	• 2.D – Physical Security
• Operations Order 5.3.01, Records Management System (RMS) Access	• 2.A – Authorization
• Operations Order 5.3.02, Computer Aided Dispatch (CAD) System Access	• 2.A – Authorization
• Criminal Intelligence Files	• 2.A – Authorization • 4.A – Training

Last Organizational Review: